

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1 1-3 (Canceled).

1 4. (Currently amended) An execution unit adapted to perform ~~at least a~~
2 ~~portion~~ a given round of the Data Encryption Standard, the execution unit
3 comprising:

4 a) a Left Half input;

5 b) a Key input;

6 c) a Table input;

7 d) a first group of transistors configured to receive the Table input, perform
8 a table look-up, and output data;

9 e) a first exclusive-or operator having two inputs and an output, the first
10 exclusive-or operator configured to receive the Left Half input and the
11 Key input;

12 f) a second exclusive-or operator having two inputs and an output, the
13 second exclusive-or operator configured to receive the data output by the

14 first group of transistors and the output of the first exclusive-or operator;
15 and
16 g) a third exclusive-or operator having two inputs and an output, the third
17 exclusive-or operator configured to receive the Left Half input and the
18 data output by the first group of transistors;
19 h) wherein the output of the second exclusive-or operator is used as the
20 Table input for the next round of the Data Encryption Standard;
21 i) wherein the output of the third exclusive-or operator is used as a Right
22 Half input for the next round of the Data Encryption Standard; and
23 j) wherein a Right Half input from the previous round of the Data
24 Encryption Standard is used as the Left Half input for the next round of
25 the Data Encryption Standard.

1 5. (Original) The execution unit of claim 4, further comprising a second
2 group of transistors configured to receive data output by the second exclusive-or
3 operator.

1 6. (Original) The execution unit of claim 4, wherein the execution unit is
2 operable to perform an exclusive-or operation for a CBC mode, a CFB mode, or
3 an OFB mode of DES encryption at the same time that the first group of

4 transistors performs one or more of the following actions: receiving the table
5 input, performing the table look-up, and outputting data.

1 7. (Currently amended) An execution unit adapted to perform ~~at least a~~
2 ~~portion~~ a given round of the Data Encryption Standard, the execution unit
3 comprising:

- 4 a) a Left Half input;
- 5 b) a Key input;
- 6 c) a Table input;
- 7 d) a first group of transistors configured to receive the Table input, perform
8 a table look-up, and output data;
- 9 e) a first exclusive-or operator having two inputs and an output, the first
10 exclusive-or operator configured to receive the Left Half input and the
11 Key input;
- 12 f) a second exclusive-or operator having two inputs and an output, the
13 second exclusive-or operator configured to receive the output of the first
14 group of transistors and the output of the first exclusive-or operator;
- 15 g) a third exclusive-or operator having two inputs and an output, the third
16 exclusive-or operator configured to receive the Left Half input and the

17 output of the first group of transistors ~~and the output of the first~~
18 ~~exclusive-or operator~~; and
19 h) a multiplexer, the multiplexer having two data inputs and an output, the
20 first of the two data inputs configured to receive the output of the first
21 exclusive-or operator, the second of the two data inputs configured to
22 receive the output of the second exclusive-or operator;
23 i) wherein the output of the multiplexer is used as the Table input for the
24 next round of the Data Encryption Standard; and
25 k) wherein the output of the third exclusive-or operator is used as a Left Half
26 input for the next round of the Data Encryption Standard.

1 8. (Original) The execution unit of claim 7, further comprising a second
2 group of transistors configured to receive data output by the multiplexer.

1 9. (Original) The execution unit of claim 7, wherein the execution unit is
2 operable to perform an exclusive-or operation for a CBC mode, a CFB mode, or
3 an OFB mode of DES encryption at the same time that the first group of
4 transistors performs one or more of the following actions: receiving the table
5 input, performing the table look-up, and outputting data.

1 10. (Currently amended) An execution unit adapted to perform ~~at least a~~
2 ~~portion~~ a given round of the Data Encryption Standard, the execution unit
3 comprising:
4 a) a Left Half input;
5 b) a Key input;
6 c) a Table input;
7 d) a Select input;
8 e) a first group of transistors configured to receive the Table input, perform
9 a table look-up, and output data;
10 f) a first exclusive-or operator having two inputs and an output, the first
11 exclusive-or operator configured to receive the Left Half input and the
12 Key input;
13 g) an AND operator, the AND operator having two inputs and an output, the
14 first of the two inputs of the AND operator configured to receive the
15 output of the first group of transistors, the second of the two inputs of the
16 AND operator configured to receive the Select input;
17 h) a second exclusive-or operator having two inputs and an output, the
18 second exclusive-or operator configured to receive the output of the AND
19 operator and the output of the first exclusive-or operator; and

- 20 i) a third exclusive-or operator having two inputs and an output, the third
21 exclusive-or operator configured to receive the Left Half input and the
22 output of the first group of transistors;
- 23 l) wherein the output of the second exclusive-or operator is used as the
24 Table input for the next round of the Data Encryption Standard; and
- 25 j) wherein the output of the third exclusive-or operator is used as a Left Half
26 input for the next round of the Data Encryption Standard.

1 11. (Original) The execution unit of claim 10, further comprising a second
2 group of transistors configured to receive data output by the second exclusive-or
3 operator.

1 12. (Original) The execution unit of claim 10, wherein the execution unit
2 is operable to perform an exclusive-or operation for a CBC mode, a CFB mode, or
3 an OFB mode of DES encryption at the same time that the first group of
4 transistors performs one or more of the following actions: receiving the table
5 input, performing the table look-up, and outputting data.

1 13-15 (Canceled).

1 16. (Currently amended) An execution unit adapted to perform ~~at least a~~
2 ~~portion of a~~ given round of the Data Encryption Standard, the execution unit
3 comprising:
4 a) a Left Half input;
5 b) a Key input;
6 c) a Table input;
7 d) a Select input;
8 e) a first group of transistors configured to receive the Table input and the
9 Select input, perform a table look-up, and output, via a first output, the
10 result of the table look-up, the first group of transistors further configured
11 to output the result of the table look-up, via a second output, if the Select
12 input is a first value, and configured to output a zero, via the second
13 output, if the Select input is a second value;
14 f) a first exclusive-or operator having two inputs and an output, the first
15 exclusive-or operator configured to receive the Left Half input and the
16 Key input;
17 g) a second exclusive-or operator having two inputs and an output, the
18 second exclusive-or operator configured to receive the result output via
19 the second output of the first group of transistors and the output of the
20 first exclusive-or operator; and

21 h) a third exclusive-or operator having two inputs and an output, the third
22 exclusive-or operator configured to receive the result output via the first
23 output of the first group of transistors and the Left Half input;
24 m) wherein the output of the second exclusive-or operator is used as the
25 Table input for the next round of the Data Encryption Standard; and
26 i) wherein the output of the third exclusive-or operator is used as a Left Half
27 input for the next round of the Data Encryption Standard.

1 17. (Previously presented) The execution unit of claim 16, further
2 comprising a second group of transistors configured to receive data output by the
3 second exclusive-or operator.

1 18. (Previously presented) The execution unit of claim 16, wherein the
2 execution unit is operable to perform an exclusive-or operation for a CBC mode, a
3 CFB mode, or an OFB mode of DES encryption at the same time that the first
4 group of transistors performs one or more of the following actions: receiving the
5 table input, performing the table look- up, and outputting data.